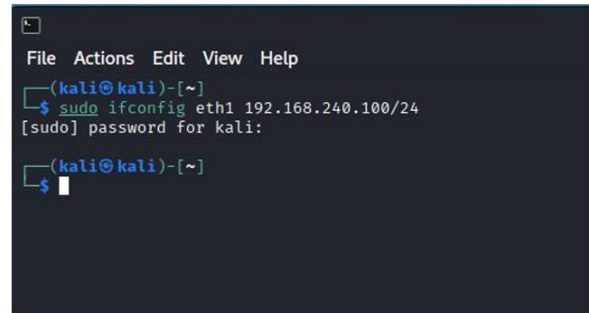
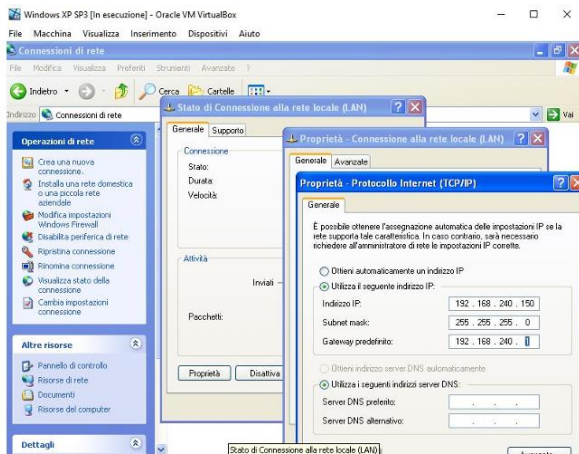
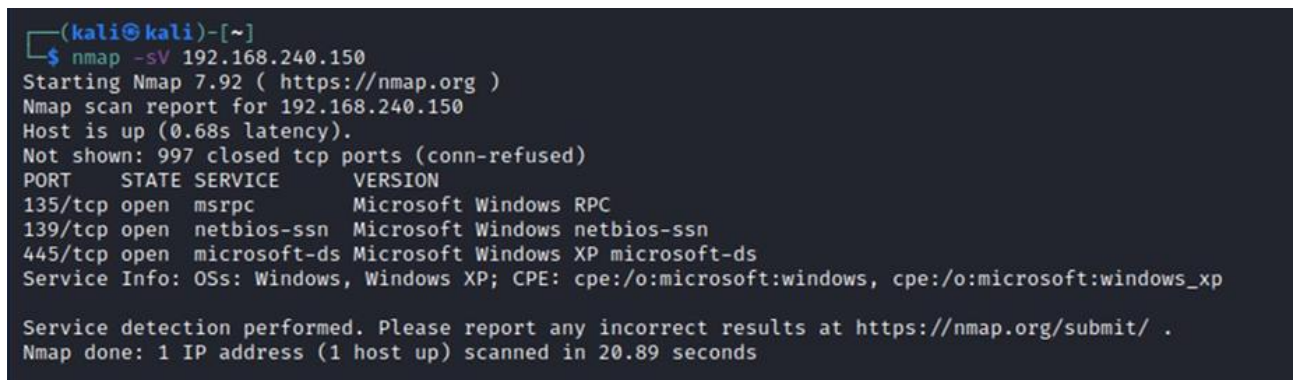


ESERCIZIO – SOLUZIONE

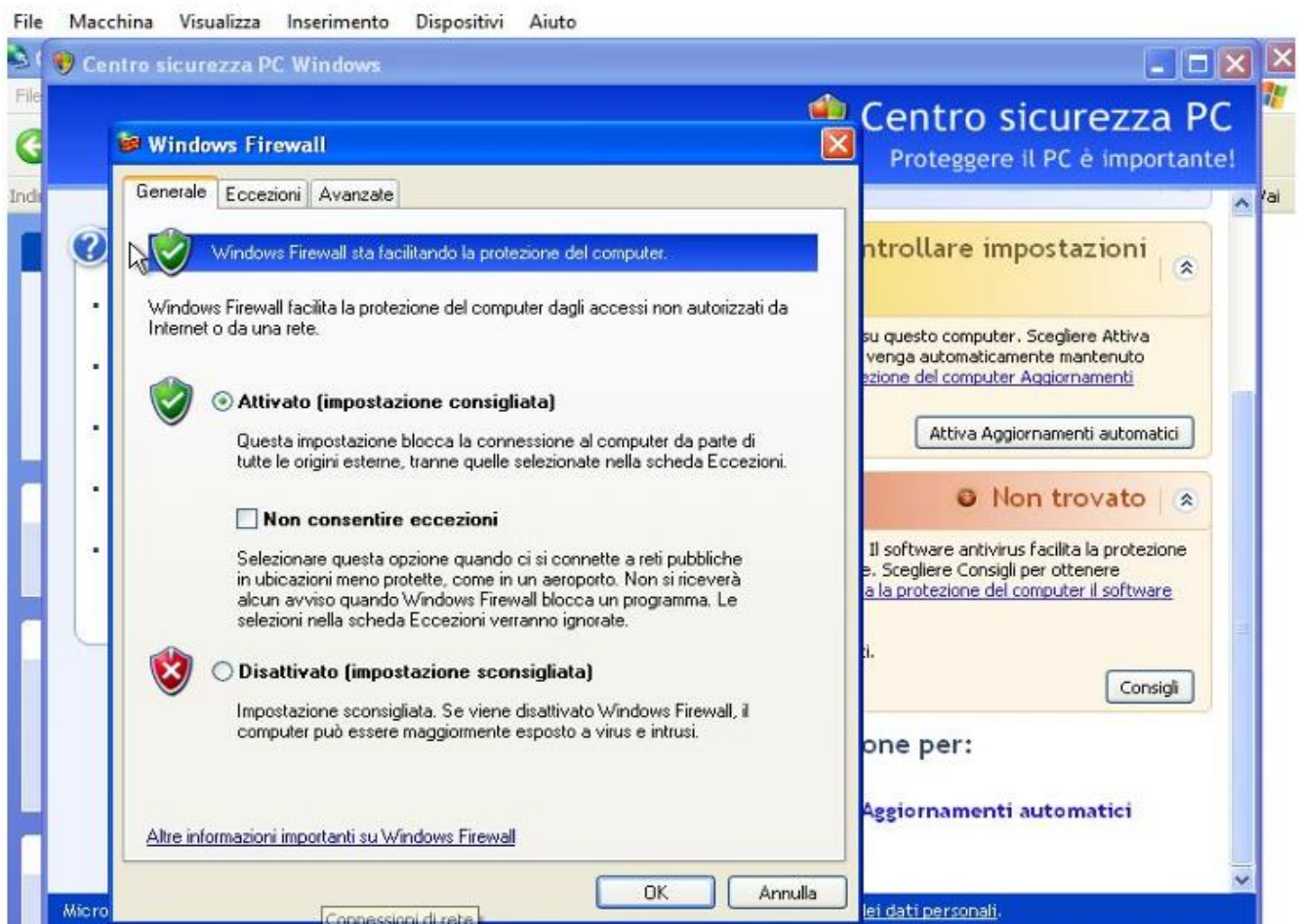
Per prima cosa, soddisfiamo i requisiti del laboratorio, impostando gli IP delle macchine come richiesto. Ricordatevi che per modificare l'IP della macchina Windows dovete seguire il percorso Connessioni di rete → stato di connessione alla rete LAN → proprietà → proprietà TCP / IP



Accertiamoci che il Firewall di Windows sia disattivato e lanciamo la scansione verso il nostro target con lo switch -sV. La scansione ci riporta 3 servizi in ascolto rispettivamente sulle porte TCP 135,139,445.



Attiviamo il Firewall di Windows XP e procediamo nuovamente alla scansione.



Il risultato della scansione ci riporta che la macchina o non è accesa, oppure se è accesa sta bloccando l'host discovery di nmap. Ci consiglia quindi di provare con il parametro `-Pn`. La situazione è piuttosto chiara, il Firewall sta bloccando il traffico in entrata con protocollo ICMP (il ping). Proviamo a sfruttare lo switch `-Pn` per evitare il ping e passare direttamente alla scansione dei servizi

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.92 ( https://nmap.org )  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.51 seconds
```

Utilizzando lo switch `-Pn`, la scansione salterà il ping e passerà alla service discovery. A questo giro tutte le porte sembrano filtrate, ovvero non hanno risposto alle richieste dello scanner. È palese che il Firewall sta bloccando l'accesso alle porte. Ricordate che una porta risulta filtrata quando lo scanner non riceve nessun segnale – in generale non si può dire con certezza se una porta filtrata sia aperta o chiusa (nella fattispecie sappiamo che sulle porte 135,139,445 sono in ascolto servizi).

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150 -Pn  
Starting Nmap 7.92 ( https://nmap.org )  
Nmap scan report for 192.168.240.150  
Host is up.  
All 1000 scanned ports on 192.168.240.150 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 215.00 seconds  
  
(kali㉿kali)-[~]  
$
```

CONCLUSIONE

L'abilitazione del Firewall di Windows XP sta di fatto bloccando la scansione dall'esterno verso i servizi attivi sulla macchina Windows XP. Sappiamo che i servizi sono vulnerabili in quanto li abbiamo sfruttati nella Unit 2 durante i nostri test con Metasploit – di conseguenza possiamo dire che il Firewall sta preventivamente riducendo rischi di attacchi dall'esterno, rendendo inaccessibili dall'esterno i servizi sulle porte 135,139,445 TCP.